EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L3	43	"380"/$.ccls. and (padd$3 with (random near number)) and ((crypt$3 cryptograph$3 encrypt$3 cipher$3 scrambl$3 decrypt$3 uncipher$3 cypher$3))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/23 11:35
L4	41	"380"/$.ccls. and (padd$3 with (random near number)) and ((crypt$3 cryptograph$3 encrypt$3 cipher$3 scrambl$3 decrypt$3 uncipher$3 cypher$3) with (string byte stream bits text))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/23 11:35
L5	15	"380"/28,30.ccls. and (padd$3 with (random near number)) and ((crypt$3 cryptograph$3 encrypt$3 cipher$3 scrambl$3 decrypt$3 uncipher$3 cypher$3) with (string byte stream bits text))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/23 11:50
L6	15	"380"/28,30.ccls. and (padd$3 with (random near number)) and ((crypt$3 cryptograph$3 encrypt$3 cipher$3 scrambl$3 decrypt$3 uncipher$3 cypher$3) with (string byte stream bits text))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/23 12:21
L7	4	"380"/28,30.ccls. and (padd$3 with (random near number)) and ((crypt$3 cryptograph$3 encrypt$3 cipher$3 scrambl$3 decrypt$3 uncipher$3 cypher$3) and (rule policy policies))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/23 11:39
L8	3	"380"/28,30.ccls. and (padd$3 with (random near number)) and ((conversion inversion) with (string byte stream bits text))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/23 11:38
L9	5	"380"/28,30.ccls. and (padd$3 with ("OAEP" "NTRU")) and ((crypt$3 cryptograph$3 encrypt$3 cipher$3 scrambl$3 decrypt$3 uncipher$3 cypher$3) with (string byte stream bits text))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/23 11:53
L10	1	(padd$3 same ("OAEP" "NTRU")) and ((crypt$3 cryptograph$3 encrypt$3 cipher$3 scrambl$3 decrypt$3 uncipher$3 cypher$3) with (string byte stream bits text)) and ((conversion converting inverting inversion) with (string byte stream bits text) with (rule policy policies specification))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/23 11:56
L11	104	(padd$3) and ((crypt$3 cryptograph$3 encrypt$3 cipher$3 scrambl$3 decrypt$3 uncipher$3 cypher$3)) and ((conversion converting inverting inversion) with (string byte stream bits text) with (rule policy policies specification))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/23 11:56

EAST Search History

L12	3	"380"/$.ccls. and (padd$3) and ((crypt$3 cryptograph$3 encrypt$3 cipher$3 scrambl$3 decrypt$3 uncipher$3 cypher$3)) and ((conversion converting inverting inversion) with (string byte stream bits text) with (rule policy policies specification))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/23 13:12
L13	14	(padd$3) and ((crypt$3 cryptograph$3 encrypt$3 cipher$3 scrambl$3 decrypt$3 uncipher$3 cypher$3) with (string byte stream bits text)) and ((conversion converting inverting inversion) with (string byte stream bits text) with (rule policy policies specification))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/23 12:06
L16	32	"713"/$.ccls. and (padd$3 with (random near number)) and ((crypt$3 cryptograph$3 encrypt$3 cipher$3 scrambl$3 decrypt$3 uncipher$3 cypher$3) with (string byte stream bits text))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/23 12:21
L17	7	"708"/$.ccls. and (padd$3 with (random near number)) and ((crypt$3 cryptograph$3 encrypt$3 cipher$3 scrambl$3 decrypt$3 uncipher$3 cypher$3) with (string byte stream bits text))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/23 12:21
L18	2	"380"/28,30,37,42.ccls. and (padd$3) and ((crypt$3 cryptograph$3 encrypt$3 cipher$3 scrambl$3 decrypt$3 uncipher$3 cypher$3)) and ((conversion converting inverting inversion) with (string byte stream bits text) with (rule policy policies specification))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/23 13:12

Terms used: **padding OAEP public key random number** Found **730** of **209,709**

Sort results by: publication date
Display results: expanded form
Save results to a Binder
Search Tips
Open results in a new window
Try an Advanced Search
Try this search in The ACM Guide

Results 41 - 60 of 200 Result page: previous 1 2 **3** 4 5 6 7 8 9 10 next
Best 200 shown Relevance scale

41 Security through the eyes of users: Hardening Web browsers against man-in-the-middle and eavesdropping attacks
Haidong Xia, José Carlos Brustoloni
May 2005 **Proceedings of the 14th international conference on World Wide Web WWW '05**
Publisher: ACM Press
Full text available: pdf(770.11 KB) Additional Information: full citation, abstract, references, index terms

Existing Web browsers handle security errors in a manner that often confuses users. In particular, when a user visits a secure site whose certificate the browser cannot verify, the browser typically allows the user to view and install the certificate and connect to the site despite the verification failure. However, few users understand the risk of man-in-the-middle attacks and the principles behind certificate-based authentication. We propose context-sensitive certificate verification (CSCV), w ...

Keywords: HTTPS, SSL, Web browser, certificate, eavesdropping attack, just-in-time instruction, man-in-the-middle attack, password, safe staging, well-in-advance instruction

42 Security evaluation of email encryption using random noise generated by LCG
Chung-Chih Li, Hema Sagar R. Kandati, Bo Sun
April 2005 **Journal of Computing Sciences in Colleges**, Volume 20 Issue 4
Publisher: Consortium for Computing Sciences in Colleges
Full text available: pdf(153.28 KB) Additional Information: full citation, abstract, references, index terms

Theoretically, using any Linear Congruence Generator (LCG) to generate pseudo-random numbers for cryptographic purposes is problematic because of its predictableness. On the other hand, due to its simplicity and efficiency, we think that the LCG should not be completely ignored. Since the random numbers generated by the LCG are predictable, it is clear that we cannot use them directly. However, we shall not introduce too much complication in the implementation which will compromise the reasons, ...

Keywords: email encryption, lightweight encryptions, linear congruential generator

43 Reviewed articles: Efficient security for IPv6 multihoming
Marcelo Bagnulo, Alberto García-Martínez, Arturo Azcorra
April 2005 **ACM SIGCOMM Computer Communication Review**, Volume 35 Issue 2
Publisher: ACM Press
Full text available: pdf(112.95 KB) Additional Information: full citation, abstract, references, index terms

☐ Search Session History

Edit an existing query or compose a new query in the Search Query Display.

Select a search number (#) to:

- Add a query to the Search Query Display
- Combine search queries using AND, OR, or NOT
- Delete a search
- Run a search

Thu, 23 Aug 2007, 1:18:19 PM EST

Search Query Display

[redacted]

Recent Search Queries

#1 ((padding<in>metadata) <and> (public key<in>metadata)) <and> (random number<in>metadata)

#2 ((padding <in>metadata) <and> (random number<in>metadata))

[redacted]

Google Patent Search BETA (pad OR padding) "random number" "public ke Search Patents Advanced Patent Sea Google Patent Search

Patents

Patents **1 - 10** on **(pad OR padding) "random number" "public key"**. (**0.12** seconds)

Tokenless identification system for authorization of electronic transactions and electronic ...
US Pat. 5613012 - Filed May 17, 1995 - Smarttouch, LLC.
If the **random number** generator is based on time of day, or on some other ...
Public Key Encryption Library **Public Key** encryption support libraries are ...

Computer systems to inhibit unauthorized copying, unauthorized usage, and automated cracking of ...
US Pat. 4558176 - Filed Sep 20, 1982
The PDU 7 will encrypt this **random number** using the common DES (or similar) ...
a command on bus 54 which causes the One Time **Pad Random Number** Generator ...

Public key cryptosystem **key** management based on control vectors
US Pat. 5200999 - Filed Sep 27, 1991 - International Business Machines Corporation
12 03 Reserved (=3 XW) 15 01 Length of Random **Pad** for Secret Part in bytes ...
Register (Pseudo-**Random Number** Seed Key #2) 144 16 CKMP Register (Current ...

Hybrid **public key** algorithm/data encryption algorithm **key** distribution method based on control ...
US Pat. 5142578 - Filed Aug 22, 1991 - International Business Machines Corporation
Key generator means 508 is a pseudo **random number** generator for generating ...
block can in the simplest case consist of the hash value 65 and **padding** data, ...

Cryptographic protocol for secure communications
US Pat. 5241599 - Filed Oct 2, 1991 - AT&T Bell Laboratories
It is tempting to finesse the issue by instead transmitting the seed of the **random number** generator used to produce the **public key**. ...

Differential work factor cryptography method and system
US Pat. 5764772 - Filed Dec 15, 1995 - Lotus Development Coporation
The recipient's system compares the resulting **pad** are encrypted with the **public key** of that second encrypted entity with the encrypted entity received with ...

Abuse-resistant object distribution system and method
US Pat. 5400403 - Filed Aug 16, 1993 - RSA Data Security, Inc.
If it is shorter, then only part of the **pad** is needed. ... Access number generation which generates a value 17 with the **random-number** generator as input, ...

Method and apparatus for **public key** exchange in a cryptographic system
US Pat. 5463690 - Filed Dec 14, 1993 - Next Computer, Inc.
These keys are referred to as a "one-time **pad**." A one-time **pad** is a key used in enciphering ... The **random number** E is the enciphering key and is public. ...

Method and apparatus for **public key** exchange in a cryptographic system
US Pat. 5159632 - Filed Sep 17, 1991 - NeXT Computer, Inc.
A one-time **pad** is a key ble to determine the private key from the **public key**.
The receiver simply executes the inverse of the trans- vate key, known only to ...

Tokenless biometric transaction authorization system

Google Patent Search BETA

padding "random number" "public key" "OAEP" Search Patents Advanced Patent Sear Google Patent Search

Patents

Patents **1** - **1** on **padding "random number" "public key" "OAEP"**. (**0.08** seconds)

Did you mean: ***adding "random number" "public key" "OAEP"***

Super secure migratable keys in TCPA
US Pat. 7242768 - Filed Jan 14, 2002 - Lenovo (Singapore) Pte. Ltd.
The **OAEP** is then XOR'ed with a **random number** to create the migratable ... 202 is then wrapped in 10 the grandparent key's **public key**. ...

padding "random number" "public key" "OAEI Search Patents

Google Patent Search Help | Advanced Patent Search

Google Home - About Google - About Google Patent Search